BUSINESS•24

ČESKÁ SPOŘITELNA

User manual

A non-stop available modern form of internet banking.

The BUSINESS 24 service
is available to you from **www.business24.cz**

BUSINESS 24 Mobile Bank
for iPhone or Android users

Telephone support of the service
in the Czech Republic: Commercial clients support at:
956 777 888
From abroad: the following phone number is available:
+420 956 777 888

TABLE OF CONTENTS

1. CHARACTERISTICS OF THE BUSINESS 24, BUSINESS 24 – LIGHT AND MOBILE BANK SERVICES 3

1.1 Principle of the service 4
1.2 Technical preconditions for the usage of the service 4
1.3 Managed accounts and cards 5
1.4 Mailing address (serves e.g. for the sending of a new security ID and password, new chip card, etc.) 6

2. ACCESS TO BUSINESS 24, COMMUNICATION AND OTHER FEES 6

2.1 Fees for access to BUSINESS 24 and Mobile Bank services 6
2.2 Fees for connecting with the telephone banker 6
2.3 Fees for BUSINESS 24 administration, etc. (other fees) 6

3. SECURITY OF THE BUSINESS 24 AND BUSINESS 24 MOBILE BANK SERVICES 6

3.1 User identification and authentication 7
3.2 Logging into the BUSINESS 24 and BUSINESS 24 Mobile Bank services 8
3.3 Blocking and unblocking access to BUSINESS 24 9

4. LIMITS USED IN BUSINESS 24 10

4.1 Account limit 10
4.2 Co-authorisation limit 11
4.3 Limit for Mobile Bank 11

5. ACCOUNT MANAGEMENT BY SEVERAL USERS 12

5.1 Authorised persons 12
5.2 Joint holder rights 12
5.3 User authorisations 13

6. ORDER PROCESSING AND CANCELLATION 13

6.1 Domestic payments system 13
6.2 Foreign payments system 14
6.3 Account operations 14
6.4 Deposit accounts 15
6.5 FX operations 15

7. USE OF BUSINESS 24 16

7.1 Via internet banking 17
7.2 Via telephone banker 17

8. BUSINESS 24 SUPPORT 17

9. IMPLEMENTING DIRECTIVE FOR THE USAGE OF ELECTRONIC CERTIFICATES IN DIRECT BANKING SERVICES 18

9.1 General provisions 18
9.2 Validity and effect of electronic certificates and chip cards 18
9.3 Electronic certificate validity renewal 19
9.4 Electronic certificate issue 19
9.5 Electronic certificate invalidation 20

10. OVERVIEW OF OPERATIONS IN THE BUSINESS 24 SERVICE 21

SEPA ERROR STATUSES 26

11. LIST OF TERMS AND ABBREVIATIONS 33

1. Characteristics of the BUSINESS 24, BUSINESS 24 – LIGHT and MOBILE BANK services

BUSINESS 24

BUSINESS 24 is an internet and telephone banking which is provided primarily to business and corporate clients of Česká spořitelna, a.s. (hereinafter referred to as the "bank") on the basis of a contract associated with the client's main/primary account (hereinafter referred to as the "account owner"), which is specified in the Contract and which may be changed.

Accounts may be serviced via the BUSINESS 24 internet banking by persons who have been set up as persons authorised to manage the accounts, so called users (hereinafter referred to as the "user"). Access to the service by phone allows not only for user support, but also for the execution of selected Administrative operations, filing of complaints and obtaining of information on executed and non-executed transactions.

BUSINESS 24 – LIGHT

The BUSINESS 24 – LIGHT service a simplified version of BUSINESS 24 and is intended **solely for corporate clients** who may use it to obtain information on the following passive transactions on accounts which have been assigned to the service:

- Display of the list and details of accounts (current, loan, deposit, savings)
- Display of passive operations on payment cards
- Display of the list and detail of bank guarantees
- Display of the list and detail of overdraft accounts
- Display of the list and detail of Credit lines
- Display of the current loan burden of the client
- Display of the account balance
- Display of the transaction history
- Display of the list of advices
- Display of the list of non-executed transactions
- Display and print of the text account statement and its export
- Display and print of the electronic statement
- Export of the data statement
- Export of the MT940 statement
- Generation of the print report for the data statement
- Contract blocking
- Contract unblocking
- Change of password
- Change of contact details
- Blocking of a user
- Application for the sending of a chip card
- Display of bank messages by type

The BUSINESS 24 - LIGHT service is governed by the same rules, principles and technical preconditions as the BUSINESS 24 service as specified below.

Should the account owner be interested in using the BUSINESS 24 service in full scope, he/she can ask for the transfer of the BUSINESS 24 – LIGHT service to BUSINESS 24 service at a business point.

BUSINESS 24 Mobile Bank

Mobile application is a service that enables you to administer your finance safely and comfortably at any time and from any place by means of a mobile telephone or a tablet with operating system iOS (iPhone, iPad, iPod touch) or Android. The application is available free of charge in the Czech and English version. At present the application is supported for operating system iOS version 6 and higher, and for Android version 4.0 and higher.

Types of managed accounts

- Current accounts
- Deposit accounts
- Savings accounts

Major features

- Displaying of account balances
- Entry of domestic payments and foreign currency payments within the bank
- Entry of FX Spot/Forward deals

- Co-authorisations of transactions (import of batch, bulk payment, single payment, foreign currency payment and express payment, foreign payment, SEPA payment, direct debit order)
- Displaying and cancellation of pending and non-executed payments
- Sending of push notifications on non-executed payments and transactions for co-authorisation
- Transaction history searching
- Display of FX tables and utilisation of exchange calculator
- Searching for Česká spořitelna ATMs and branches
- Our important contact details

Conditions

- Account in Česká spořitelna (see the Types of managed accounts) with joint holder rights A (active),P (passive), S (joint co-authorisation) or E (separate co-authorisation),
- Active BUSINESS 24 Internetbanking or BUSINESS 24 LIGHT for the set-up of password for Mobile Bank,
- Contract on higher security,
- Option to log into B24 IB also with the client number and password.

1.1 Principle of the service

Users log into the BUSINESS 24 service at www.business24.cz.

The BUSINESS 24 service also allows for the **use of telephone banker support**. (chapter 7.2 Via telephone banker and chapter 8 BUSINESS 24 support refer).

1.2 Technical preconditions for the usage of the service

The recommended equipment for the proper functionality of the SERVIS 24 Internetbanking application is a personal computer with operating system and internet browser installed:

Supported operating system versions	Supported browser versions
Microsoft Windows 7 (SP1)	Microsoft Internet Explorer 10 Microsoft Internet Explorer 11 Mozilla Firefox (last 3 versions) *) Google Chrome (last 3 versions) *)
Microsoft Windows 8 Microsoft Windows 8.1	Microsoft Internet Explorer 10 Microsoft Internet Explorer 11 Mozilla Firefox (last 3 versions) *) Google Chrome (last 3 versions) *)
Mac OS X 10.9 (Mavericks) Mac OS X 10.10 (Yosemite)	Safari 6 and higher Mozilla Firefox (last 3 versions) *) Google Chrome (last 3 versions) *)
Linux distribution CentOS version 6 and higher Linux distribution Ubuntu version 12.10 and higher	Mozilla Firefox (last 3 versions) *) Google Chrome (last 3 versions) *)

*) The latest browser versions are tested following their release for the period of 3 months and the application is adopted to them in order to safeguard full functionality and proper display.

The BUSINESS 24 Internetbanking application requires a browser capable of processing websites according to the following standards:

- HTML 4.01 (as per recommendation W3C HTML 4.01 Specification and the ISO/IEC 15445:2000 standard),
- JavaScript (as per recommendation ECMAscript-262, rev.3),
- CSS 3 (as per recommendation W3C CSS3 Values and Units),
- HTTP 1.1 (as per recommendation IETF RFC2616),
- TLS 1.0.
- The storing of cookies has to be allowed.

Usage of cookies and similar technologies
On its website and in its Internetbanking, Česká spořitelna uses small text files - cookies, which are sent to your browser. This facilitates your visits to our website and provides you with more relevant content.
These files are used particularly to save your settings, such as your preferred language, for the monitoring of the website usage rates, and the selection of proper communication. Personal data protection principles are always carefully observed.

What specific cookies are used
Personalisation – for the identification of the preferred language and login method
Authentication – to verify the user for security reasons
Technical – to safeguard communication with the bank's system and minimum parameters necessary for the operation of the application
Communication – to display multimedia content
Statistical – to determine the usage rates of application sections

Other operating systems and internet browsers may not be fully compatible with the BUSINESS 24 service, and therefore the bank cannot guarantee that the service will be displayed properly and that all of the offered functions will be processed without errors.

1.3 Managed accounts and cards

The BUSINESS 24 service may be used for the management of accounts and payment cards which are assigned to it either automatically or manually (by the authorised person).

Removal of accounts and payment cards from the BUSINESS 24 service is sometimes executed also automatically, but in most cases they are removed by the authorised person.

Adding an account and card:

- After first login, the BUSINESS 24 service will be **automatically** activated for the main/**primary account** specified in the contract for the authorised person and the **card account**, if it has been set up for the same account owner as the main/primary account. Concurrently with these accounts, all **payment cards** issued for these accounts will be automatically added to the BUSINESS 24 service.
- **Other current, savings or card accounts are added** to the service by the authorised person via the BUSINESS 24 service. Only those accounts which are identified by the contract as the client's accounts may be added. Together with the current or card account, payment cards issued for the account will be added as well.
- **A payment card holder** who is not at the same time the authorised person may add only **his/her own card.** This

card will be added to this user automatically only upon first-time login to the BUSINESS 24 service.

– For corporate clients, newly provided **loans, credit lines, bank guarantees** and newly opened **deposits accounts** are **automatically** added to the BUSINESS 24 service.
– All joint holders with passive rights in respect of at least one current accounts added to BUSINESS 24 will be automatically assigned with passive rights in respect of deposit accounts added in this manner.
– The right to view loans of corporate clients will be set up by the authorised person via the "Loans – Exchange of Documentation" activity settings, and subsequently through the settings of passive rights for individual loan accounts both for himself/herself and for other joint holders. Loans of business clients will be added to the service by the authorised person via the BUSINESS 24 service, and subsequently the authorised person will set up the rights for other joint holders.
– Loans of business clients are assigned under the service by the authorised person by means of BUSINESS 24.

Removing an account or card:

- The Main/Primary account cannot be removed.
- For corporate clients, closed deposit accounts, closed loans, credit lines and cancelled bank guarantees will be **automatically** removed. It will not be possible to manually remove or add loans, credit lines, and bank guarantees from/to the BUSINESS 24 service. Nevertheless, the client will be able to manually remove or add joint-holder rights to individual joint holders.
- For business clients closed loans will be removed automatically.
- A payment card may be removed by its holder or by the authorised person. Upon card removal by its holder, the authorised person will still be able to see the card. If the card is removed by the authorised person, the card holder will still be able to see the card.
- A removal of a current or card account will result in the removal of payment cards issued for the account.
- Card accounts may be removed by the authorised person. Only if the card account is cancelled, it will be removed automatically together with all cards issued for it.

1.4 Mailing address (serves e.g. for the sending of a new security ID and password, new chip card, etc.)

It may be changed only by an authenticated user, either through the BUSINESS 24 service, telephone support or at any business point.

The change of mailing address takes effect immediately.

2. Access to BUSINESS 24, communication and other fees

The following fees may be associated with the usage of the BUSINESS 24 service:

2.1 Fees for access to BUSINESS 24 and Mobile Bank services

Internet connection: communication fees for internet connection as per the pricelist of the connection provider.

2.2 Fees for connecting with the telephone banker

Telephone fees during contact with the telephone banker on the support line: as per the price list of the specific operator.

2.3 Fees for BUSINESS 24 administration, etc. (other fees)

Fees for the administration of the BUSINESS 24 service (monthly fee for service maintenance, fee for client certificate and reader and for the repeated sending of security data, where applicable, etc.) these are charged from the client's main/primary account specified in the contract on BUSINESS 24.

3. Security of the BUSINESS 24 and BUSINESS 24 Mobile Bank services

The BUSINESS 24 service is secured the following with security features of direct banking:

- The client number which forms part of the User set-up protocol
- Telebanking password which is included in the security consignment
- Security ID which forms part of the security consignment
- Client Certificate (so called electronic signature)

- System certificate (only for the Databanking service)
- Login SMS message (an optional enhancement of the Internetbanking security).

The following phone number is available to clients who wish to report any loss or theft of security data:

- 956 777 888 (on working days from 7:00 a.m. to 6:00 p.m.),
- 800 207 207,
- or at 956 777 956.

Other features enhancing the security of the service include the following options:

Hints for the client:

- change of access passwords (see below),
- change of limit amounts (see below),
- defining access to the contract only using the Client Certificate for individual joint holders,

Bank's security features:

- recording and archival of any communication maintained via BUSINESS 24 (in the bank systems),
- active use and combining of the security features (changes of password, limits, or the use of Client Certificate where applicable),
- logging out the client automatically if the time of validity of the site expires.
- pulling the chip card from the chip card reader and reinserting it again when logging into the BUSINESS 24 application by Client Certificate or in case of a longer inactivity in the BUSINESS 24 application.

The security data are provided by the bank to the client automatically upon opening the BUSINESS 24 service.

The Client Certificate is provided by the bank upon the user's requirement at the business point.

The user may apply for the **Client Certificate** for BUSINESS 24 either at the time of contracting the service or any time later, but only via a business point. The validity of the Client Certificate is one year. The user can renew the Client Certificate via the BUSINESS 24 Internetbanking service.

BUSINESS 24 Mobile Bank is secured through the following security features:

- Use of multi-level security – first-time login is performed by combination of internet banking security elements with the password for mobile bank
- Utilisation of software certificate
- Automatic logoff in case of idleness
- Option for shake out logoff
- Detection of non-standard set-up of the operating system

Automatic blocking in case of repeated incorrect login (3 attempts)

3.1 User identification and authentication

The precondition for performing active as well as passive transactions in respect of the account is the user's identification by means of the security features. General information on the services provided by the bank's financial group is accessible without authentication.

The following security features are used to authenticate the user:

- **Client number**
  A ten-digit number which is specific in the User set-up protocol. The User set-up protocol is given to each user when the service is contracted. The client number serves for the purposes of the client's authentication upon login. It is possible to apply for a change of the client number through a business point.
  If the user logs into the BUSINESS 24 service by Client Certificate, the appropriate client number will be displayed in the Settings menu.

- **Telebanking password**
  A six-digit number which the user has received at a business point of the bank or via registered mail for personal delivery and which serves for the client's authentication when communicating with the telephone banker and for the first-time login to the BUSINESS 24 service
  The client can change the Telebanking password via the automatic voice response service.
  In cases of lost or forgotten password, it is possible to set up a new password via the BUSINESS 24 service if the client has logged in via the Client Certificate. .
  When talking to the telephone banker the user can apply for the generation of a new password for Telebanking. For it to be sent, it is necessary to provide the required positions from the security ID.
  A client may request the generation of new security data also at a business point of the bank.

- **BUSINESS 24 Internetbanking access password**
  The password is a combination of numerals and letters of the client's choice of at least 8 and no more than 30 characters (distinguishing between upper and lower case and without the use of diacritical symbols) which should contain at least two letters and at the same time at least two numerals. The user defines his/her password when

logging into the BUSINESS 24 service for the first time, when the current password for Telebanking is used. It is possible to can change this password at any time following an authenticated login to the BUSINESS 24 service.
In case of forgotten password for BUSINESS 24, it is possible to call the telephone banker and ask him/her (after an authenticated login) to set up this password for a password identical to the Telebanking password. When the user logs in again to the BUSINESS 24 service he/she will define his/her password for BUSINESS 24. If the user has logged in via Client Certificate, it is possible to set up a new password in place of a lost or forgotten one via the BUSINESS 24 service.

- **Password for Mobile Bank**
  First login is performed by means of a Client Number, Single-use code and Password for Mobile Bank. Single-use code can be obtained in the internet banking where the Client Number will be also displayed to you. Password is a combination created by you consisting of letters without diacritical signs, numerals and some other characters. Password for Mobile Bank is created in the internet banking after login through the Client Certificate and its necessary for activation and subsequent logins to the BUSINESSIS 24 Mobile Bank application. The password must contain the minimum of 6 and the maximum of 20 characters. Password distinguishes between the lower case and upper case letters. The password must not contain simple numeric series. Brief notification will be displayed on the screen if the Caps Lock key is activated.

- **Security ID**
  An eight-digit number of which only four characters selected randomly by the system are always entered. The user can have only one valid security ID. Corporate clients can ask for repeated generation of the security ID at a business point. Corporate clients as well as business clients may apply for a new security ID via the telephone banker. The new security ID will be sent to you via registered mail for personal delivery to the client's mailing address.
  The security ID is required in particular upon first-time login to the certificate administrator and upon first-time login to the service (unless the Client Certificate is used).

- **Client Certificate**
  It is necessary for the authorisation of all entered active financial transactions and administrative operations. It is stored in a chip card and access to it is protected by a four-digit PIN code.
  To obtain the Client Certificate, you have to sign the Higher-type security protocol at any business point.

- **Login SMS**
  An optional enhancement of security (client number and password) of the BUSINESS 24 service via a login SMS message is required upon each login. The set-up of login SMS messages is performed via the BUSINESS 24 service if the client has set up a mobile phone number for the sending of security SMS messages or upon login to the service via Client Certificate. The set-up may be requested at any business point.

- **Important notices:**
  Disclosure of the aforementioned security features may jeopardise the security of data administered by the BUSINESS 24 service. It is advisable not to disclose the special registered mail consignment or individual security features to anybody and to protect them from loss or theft.
  When using the BUSINESS 24 service at computers which are not under the client's direct control, e.g. in public premises (internet cafés, office or school computer networks), it is necessary to use the login SMS for logging in.
  On its part, the bank is obliged to carry out all measures to safeguard the security of all systems and processes which secure the operation of direct banking services from the possibility to obtain the client's security data by unauthorised persons from the bank systems and records. The client will be informed of the implemented security measures. Nevertheless, the bank is not responsible for the disclosure of security data if these are disclosed on the part of the client or person selected by the client for use of the BUSINESS 24 service.
  PDF files sent via e-mail are secured with a digital signature, which will allow the client to check that the e-mail has been generated in the bank and has not been altered by any third party.

3.2 Logging into the BUSINESS 24 and BUSINESS 24 Mobile Bank services

The usage of the BUSINESS 24 service is conditioned by a login which serves for the identification and authentication of the user.

The BUSINESS 24 service requires a mandatory login via Client Certificate for all active financial transactions and administrative operations. This practically means that if the user wishes to execute any transaction or operation which will result in a change to the administered account balance or which will change the original set-up of the given account, he/she has to login using the Client Certificate.

Passive transactions (checking the balance, transaction history, etc.) and the entry of transactions for co-authorisation may be implemented even after login via the client number and password, or the login SMS where applicable.

The security set-up may be also changed to require the user to log in via Client Certificate at each time, i.e. not only when conducting active financial transactions and administrative operations, but also upon each login to the application. This set-up, however, thereafter excludes the possibility to log in via the Mobile Bank BUSINESS 24 mobile application.

3.2.1 Login via client number and password or login SMS procedure

First-time login

When login screen of the BUSINESS 24 application comes up from the internet address **www.business24.cz**, the client will be asked to enter the client number and Telebanking password (fields “Client number” and “Password”). Once the data are submitted, the system will detect that this is a first-time login and the client will be

asked to enter four randomly selected characters from their security ID and will define their password for Internetbanking (see section 3.1 User Identification and authentication – entry password for the BUSINESS 24 Internetbanking service).

The security ID and Telebanking password is specified in a special registered mail consignment which the client receives by post for personal delivery after you have contracted the BUSINESS 24 service. The client number forms part of the User set-up protocol.

Second and subsequent logins

To log in, it is necessary to use the client number and current password for BUSINESS 24, and the login SMS code, if applicable.

3.2.2 Procedure for login via client certificate

First-time login

Before first-time login, it is necessary to install the necessary components. The installation package is available from the csas.cz website, under the Downloads section (https://www.csas.cz/PKIInstall).

Upon the first-time login to BUSINESS 24 it is possible to activate the Client Certificate even if the client has not previously logged in using the client number and Telebanking password. It is possible to do so on the login screen of BUSINESS 24 through the "Certificate administrator – entry into application" option

In this case the client only inserts the chip card into the reader connected to the computer and selects the appropriate option from the login screen. Thereafter the client will be prompted to enter the PIN for the chip card. This PIN is provided in the envelope together with the chip card, which the client has received after the conclusion of the Higher-type security protocol at a business point. Following the entry of the PIN, the client is redirected to the entry of 4 randomly selected characters from the security ID. The security ID is specified in a special registered-mail letter which is delivered by post to the client's own hands when the BUSINESS 24 service is contracted.

Second and subsequent logins

To log in, the client uses the activated client certificate. The user inserts the chip card to the reader connected to the computer. Once the client selects the appropriate option on the login screen, he/she will be prompted to enter the PIN code for the chip card.

For more details for login through client certificate please refer to the Client Certificate Manual.

3.2.3 Procedure for login to BUSINESS 24 Mobile Bank

First-time login

First-time login via a mobile phone or tablet is performed by means of a Client Number, Single-use code and Password for Mobile Bank. Single-use code can be obtained in the internet banking where the Client Number will be also displayed. The password for Mobile Bank is created in the Internetbanking following login via the Client Certificate and its necessary for activation and subsequent logins to the BUSINESSIS 24 Mobile Bank application. Concurrently, when activating the BUSINESS 24 Mobile Bank, the client also selects a password for a repository which serves of the confirmation of active operations.

Second and subsequent logins

To log in you will have to use the current password for BUSINESS 24 Mobile Bank.

3.3 Blocking and unblocking access to BUSINESS 24

3.3.1 Blocking user access

Blocking a user upon own request

Blocking upon own request may be performed through the telephone banker.

Blocking user if incorrect client number and password are entered

Only three attempts for the entry of security data which comprise of the client number and Telebanking or Internetbanking password have been set up. If the client enters an incorrect password with the client number for three times in a row, his/her access to BUSINESS 24 will be blocked. If the client is also a user of the SERVIS 24 services, access to the SERVIS 24 services will be blocked as well.

An incorrect entry of the client number means an entry of a number other than the one which is specified in the User set-up protocol, which the client has received at the business point or in a consignment sent to the mailing address.

The entry of an incorrect password is an entry of a password other than the Telebanking or Internetbanking password which has been set up upon the last successful change. Upon successful login the login attempts are reset to zero.

Blocking if the Client Certificate is invalid or if the PIN for chip card has been entered incorrectly

The usage of the Client Certificate requires, for security reasons, its regular renewing (the certificate expires after one year). If the client fails to renew the Client Certificate within the specified timeline, it will be automatically invalidated. If the user wishes to continue using the Client Certificate, he/she has to apply for the issue of a new one at a business point where an Application for higher type of security will be drafted with the client. The client will obtain a password allowing to obtain the Certificate on the basis of which it is possible to re-activate the Certificate.

Three attempts for the entry of the PIN for chip card have been set up. After three unsuccessful attempts access to the chip card will be blocked. To unblock the access it is necessary to use the PUK code which the client has received together with the chip card in a special envelope. If the client enters an invalid PUK code seven times in a row, access will be blocked and a new card has to be issued for the client via a business point.

Revoking the validity of Client Certificate

The client himself/herself may apply for the revocation of Client Certificate after he/she logs in to the BUSINESS 24 service or via a business point or via the support line at 956 777 888 (on working days from 7:00 a.m. to 6:00 p.m.).

The validity of the client Certificate invalidated upon own request of the client cannot be renewed. If the client wishes to continue using the Client Certificate, he/she has to apply for the issuance of a new certificate at a business point.

Blocking the security ID

Only three attempts for the entry of the security ID have been set up. If the client enters an incorrect security ID three times in a row, it will become blocked. It is not possible to unblock the security ID, the client will always have to apply for the generation of a new security ID via a business point or a telephone banker. If the client applies via a business point, the new security ID will be generated and provided to him/her immediately. If he client applies via the telephone banker, the new security ID will be sent to him/her by registered mail consignment for personal delivery to the client's mailing address.

3.3.2 Unblocking user access

The client can perform the unblocking of access to the BUSINESS 24 service via a telephone banker or via the BUSINESS 24 service if he/she logs in through the Client Certificate (unblocking via the PUK code). If the client is also a SERVIS 24 user, access to these services will become unblocked as well. The only exception is blocking of access through the Client Certificate and blocking of the security ID which may be unblocked only by a personal visit to a business point.

If the user blocks his/her access to the entire BUSINESS 24 service he/she can unblock it by applying for the generation of new security data which will be sent to him/her to the entered mailing address for BUSINESS 24.

After unblocking, the current set-up of the client's user roles for accounts will be restored.

3.3.3 Blocking the client (contract)

A user or the authorised person may apply for the blocking of client via the telephone support, the BUSINESS 24 service or via a business point.

3.3.4 Unblocking the client (contract)

The client may be unblocked solely by the authorised person of the given client, via the telephone support, the BUSINESS 24 service or via a business point.

3.3.5 Blocking the access to the BUSINESS 24 Mobile Bank application

It is possible to block the access to the BUSINESS 24 Mobile Bank application via Internetbanking or Telebanking but also in the event you enter the password for Mobile Bank incorrectly, three times in a row.You can also use the Deactivate button on the login page of the application or in the application menu after you are logged in.

3.3.6 Unblocking the access to the BUSINESS 24 Mobile Bank application

You can unblock the access to the BUSINESS 24 Mobile Bank application only via Internetbanking, where you have to set the password for Mobile Bank again and to generate the single-use code.

4. Limits used in BUSINESS 24

4.1 Account limit

This is the maximum daily amount of active transactions which may be entered and submitted for processing from the given account within the scope of the BUSINESS 24 service on a business day.

It is an optional limit which may not be exceeded on the given day, not even if you are using the Client Certificate.

The account limit is automatically preset to 100 000 000 CZK (in words: one hundred million Czech crowns) with the possibility to increase it up to 10 000 000 000 CZK (in words: ten billion Czech crowns), or to decrease it via the BUSINESS 24 service. The limit may be adjusted (decreased or increased) only by the authorised person using a Client Certificate. The limit is not affected where active transactions conducted between the accounts of a single owner assigned under BUSINESS 24, which are also assigned to the user who performs the transaction, are concerned. (For example, if two current accounts are assigned under one contract the limits are not affected by transfers of money between those accounts).

In respect of foreign-currency accounts, the limits are set as equivalents of the amounts in CZK as per the current FX rate of the account currency at the time of posting the required transaction. Limits are recalculated using the non-cash/buy rate.

The limits are zeroised every day at 11:00 p.m.

4.1.1 Detailed description of setting up the account limit

1. In the “SETTINGS” tab, select the “ACCOUNT SETTINGS” option from the left menu and then the “Set up account limit” option.
2. In the “List of account limits” screen select the account for which limits are to be set up.
3. The “Change account limit – step 1 of 2” screen will come up. If you wish to set up the limit for the maximum amount of transactions performed per day for the account, enter the required amount in the “New limit” field.
4. If you wish the confirmation of transaction acceptance to be delivered to you, complete the “By e-mail” field and select “Continue”.
5. The “Change account limit – step 2 of 2” screen will come up. Check the entered details and select “Send” to confirm.
6. The “Transaction acceptance confirmation” screen will be displayed.

If the current value of the account limit has been set up to “not defined”, the daily limit on this account will be 100 million CZK.

4.2 Co-authorisation limit

This is the maximum total daily amount of active transactions which may be executed by users on the given account without the necessity of being authorised by another account joint-holder. Above-limit transactions have to be authorised (co-authorised) by other account joint holders. The co-authorisation limit is set up and may be changed only through the BUSINESS 24 service by the authorised person, for each account separately. It is an optional component of money transfers security and it cannot be exceeded, not even if the Client Certificate is used.

The limits are zeroised every day at 11:00 p.m.

These limits are not applicable to transactions between accounts belonging to a single user and falling under a single “Contract on the provision of BUSINESS 24“.

4.2.1 Detailed description of setting up co-authorisations

1. In the “SETTINGS” tab, select the “USER SETTINGS” option from the left menu and then the “Set up co-authorisation” option.
2. In the "List of co-authorisation settings” screen, select the account in respect of which co-authorisation is to be set up.
3. The “ Change co-authorisation set-up – step 1 of 2” screen will come up. Select “Yes” for “Set up co-authorisation”, enter the amount from which transactions are to be approved by several joint holders in the “Co-authorisation limit” field, (if each transaction is to be co-authorised by several joint holders, enter 0), and enter the number of joint holders who have to co-authorise a transaction for it to be processed in the “Number of co-authorisations” field.
4. If you wish the confirmation of transaction acceptance to be delivered to you, complete the “By e-mail” field and select the “Continue” field.
5. If you wish the confirmation of transaction acceptance to be delivered to you, complete the “By e-mail” field and select the “Continue” option.
6. In the “Change co-authorisation set-up – step 2 of 2” screen, check the entered details and select “Send” for confirmation.
7. On the next “Transaction acceptance confirmation” screen, select the “Continue to set up co-authorisation” option and repeat steps 2 – 5 for all accounts for which co-authorisation is to be set up.

4.3 Limit for Mobile Bank

The limit is set per user at 5 million Czech crowns per one day. The limit is taken into consideration at the point hen the transaction is sent out from the transaction repository.

5. Account management by several users

The BUSINESS 24 service allows for the assigned bank accounts and selected functionalities without the account context to be administered by several users. For each of them, specific rights for the given account management may be set up (e.g. only viewing of transactions). For the user to be able to administer accounts via BUSINESS 24, he/she has to be included in the specimen signatures for the account. In respect of selected functionalities without the account context, joint holders are assigned by the decision of the authorised person.

In the contract the client himself/herself defines one or more users who will set up the rights of managing the account via BUSINESS 24 for individual **joint holders**. The user who sets up these rights for joint holders is called the **authorised person.**

5.1 Authorised persons

There may be an unlimited number of **authorised persons** for the contract. For the scope of the BUSINESS 24 service, joint acting of authorised persons may be defined, which means that each administrative operation has to be jointly authorised by the defined number of authorised persons. After the administrative operation is created, it is stored in so called administrative operations repository where it awaits authorisation by other authorised persons. If the operation is not authorised by the necessary number of authorised persons within thirty days of its creation it will become invalid.

Joint handling by authorised persons is not applicable to active card operations.

A client – natural person, who concludes the contract, is automatically assigned the role (rights) of the authorised person without the option to cancel this set-up. If the client concludes the contract for a legal person, the account owner (statutory representative) does not need to be the authorised person, and may appoint other persons to assume this role.

If the authorised person is specified for the accounts of the given client assigned under BUSINESS 24 also on the specimen signature, it will have automatically all rights for the handling of money on the accounts of the given client, i.e. the right to conduct active transactions, passive transactions and joint co-authorisations which may be changed to independent co-authorisation.

The set-up of rights for activities requires a power of attorney for the authorised person and subsequent electronic authorisations for other users in BUSINESS 24.

The authorised person is authorised to perform the following administrative transactions:

- add an account;
- remove an account;
- enter an account name;
- set up an account limit;
- apply for the opening/change of a current account;
- open/change a deposit account;
- set-up access to contract;
- block the contract;
- unblock the contract;
- set-up co-authorisation parameters;
- set-up data statements;
- activate/deactivate/change statement series (for Business Clients);
- set-up the sending of advices;
- perform joint holder/users administration;
- perform sponsored person administration;
- apply for cheque issuance;
- apply for debit card issuance;
- apply for the provision of a bank reference on the authorised person himself/herself;
- apply for the set-up of a balance regulation standing order;
- apply for loan drawdown;
- submit templates;
- display documents sent via BUSINESS 24.

5.2 Joint holder rights

The following rights (or combination thereof) may be set up for **users – joint holders:**

- **Active transactions (A) right** – the joint holder may enter transactions associated with transfers of money from the given account or send payment instructions files for collection accounts.
- **Passive transactions (P) right** – the joint holder has access to information associated with the given account (e.g. the account balance).
- **Joint co-authorisation of transactions (S) right** – the joint holder may co-authorise (authorise) transactions which have exceeded the co-authorisation limit (chapter 4.2 Co-authorisation limit refers) and which are stored in the repository of transactions awaiting co-authorisation. One co-authorisation of this joint holder increases the current number of co-authorisations by one.
- **Exclusive co-authorisation of transactions (E) right -** the joint holder may co-authorise (authorise) transactions which have exceeded the co-authorisation limit (chapter 4.2 Co-authorisation limit refers) and which are stored in the

repository of transactions awaiting co-authorisation; a single co-authorisation of this joint holder substitutes all missing co-authorisations and the transaction is subsequently sent for processing.

- **Entry of transactions to the repository of transactions awaiting co-authorisation (T) right –** the joint holder may only enter transactions which are sent to the repository of transactions awaiting co-authorisation, where they await authorisation by a joint holder E or by the necessary number of joint holders S.
- **Payment card administration (K) right–** the joint holder may carry out active operations with the cards.

The individual user rights may be combined. Their specification is provided in chapter 10 List of BUSINESS 24 operations (Tab. 1). For better orientation, the individual types of joint holders are identified with the letters A, P, S, E, T, and K.

A single user may be the authorised person and a joint holder at the same time.

The authorised person is automatically maintained as the joint holder with the A, P, S rights (with the possibility to change S to E) and the K right.

The T right may be set up only if co-authorisation has been set up for the account.

5.3 User authorisations

In respect of Electronic pledge of receivables, Bank guarantees, Documentary deals, Exchange of contractual documentation, and Confirmation of Treasury deals operations, users may be assigned authorisations to perform activities with the A, P, S, E, and T rights. The set-up of the authorisation to perform activities does not require the user to be listed in the specimen signature. The authorised person who can set up authorisations for the Electronic pledge of receivables, Bank guarantees, Documentary deals, Exchange of contractual documentation activities for other users has special authorisations established by the contract. The right to set up the authorisation for the Confirmation of Treasury deals activity is automatically assigned to authorised persons in respect of the Contract on the provision of the B24 service for clients who have concluded a contract with Dealing.

6. Order processing and cancellation

The payments are processed within timelines and according to priorities detailed in the Information on Payment Service (corporate and business clients), which is available from our website (www.csas.cz under the section: Downloads / Obligatory information/ Business Terms and Conditions / Information on payment services for business and corporate clients.

6.1 Domestic payments system

6.1.1 Domestic payments system – Corporate Clients

Types of domestic payment orders/payments	**Time of transaction entry**	**Date of order submission for processing**
Individual payments entered and signed by Client Certificate(s)	Business day before 10:00 p.m.	D
Individual payments entered and signed by Client Certificate(s)	Business day after 10:00 p.m.	D+1
Express payments entered or imported and signed by Client Certificate(s)	Business day before 14:00 p.m.	D
Express payments entered and signed by Client Certificate(s)	Business day after 14:00 p.m.	D+1

6.1.2 Domestic payments system – Business Clients

Types of domestic payment orders/payments	**Time of transaction entry**	**Date of order submission for processing**
Individual payments entered and signed by Client Certificate(s)	Business day before 11:00 p.m.	D
Individual payments entered and signed by Client Certificate(s)	Business day after 11:00 p.m.	D+1
Express payments entered or imported and signed by Client Certificate(s)	Business day before 14:00 p.m.	D

6.2 Foreign payments system

6.2.1 Foreign payments system – Corporate Clients

Types of foreign payment orders	Time of transaction entry	Date of order submission for processing
Foreign payments entered with Express priority (BGN, DKK, GBP, HRK, HUF, CHF, CHF, PLN, NOK, RON, SEK)	Business day before 11:00 a.m.	D
Foreign payments entered with Express priority (EUR,CZK,USD,CAD)	Business day before 2:00 p.m.	D
Foreign payments entered with Urgent priority	Business day before 4:30 p.m.	D+1
Foreign payments entered with Standard priority	Business day before 4:30 p.m.	D+2
Prieuro payments[1]	Business day before 11:00 a.m.	D
SEPA payments entered with Express priority	Business day before 2:00 p.m.	D
SEPA payments entered with Standard priority	Business day before 4:30 p.m.	D+1
FIT payments and Payments to Slovenská spořitelna, a.s. in EUR or CZK[2]	Business day before 3:00 p.m.	D
Foreign-currency payments within the bank	Business day before 3:00 p.m.	D

6.2.2 Foreign payments system – Business Clients

Types of foreign payments	Time of transaction entry	Date of order submission for processing
Foreign payments entered with Express priority (BGN, DKK, GBP, HRK, HUF, CHF, CHF, PLN, NOK, RON, SEK)	Business day before 11:00 a.m.	D
Foreign payments entered with Express priority (EUR,CZK,USD,CAD)	Business day before 2:00 p.m.	D
Foreign payments entered with Urgent priority	Business day before 4:30 p.m.	D+1
Foreign payments entered with Standard priority	Business day before 8:00 p.m.	D+2
Prieuro payments[1]	Business day before 11:00 a.m.	D
SEPA payments entered with Express priority	Business day before 2:00 p.m.	D
SEPA payments entered with Standard priority	Business day before 8:00 p.m.	D+1
FIT payments and Payments to Slovenská spořitelna, a.s. in EUR or CZK[2]	Business day before 3:00 p.m.	D
Foreign-currency payments within the bank	Business day before 11:00 p.m.	D

[1] **Prieuro payment** – a payment in the EUR currency which is executed from the payer account to the payee account within four hours of the moment the payer submits the order to his/her bank (the order has to be without errors and the payer account has to have sufficient funds to cover the payment). Hence the payee will receive the money on the very day it was sent by the payer. Prieuro payments may be performed for payees from banks supporting this type of service.

[2] **FIT Payment -** payment in EUR to an account of a client of an ERSTE GROUP

6.3 Account operations

6.3.1 Account operations – Corporate Clients

Types of account operations	Time of transaction entry	Date of order submission for processing
Set up/change/cancel TPRZ	Business day before 2:30 p.m.	D
Set up/change/cancel TPRZ	Business day after 2:30 p.m.	D+1
Set up/change/cancel SI[1]	Business day before 3:00 p.m.	D
Set up/change/cancel SI	Business day after 3:00 p.m.	D+1
Set up/change/cancel TPÚ, TPI	Business day before 10:00 p.m.	D+1
Set up/change/cancel TPÚ, TPI	Business day after 10:00 p.m.	D+2

[1] Note: Direct debits for SIPO payments may be set up only from a sporogiro account, Czech Post does not execute direct debit payments from current accounts.

6.3.2 Account operations – Business Clients

Types of account operations	Time of transaction entry	Date of order submission for processing
Set up/change/cancel SI, TPÚ[1]	Business day before 11:00 p.m.	D
Set up/change/cancel SI, TPÚ	Business day after 11:00 p.m.	D+1

[1] Note: Direct debits for SIPO payments may be set up only from a sporogiro account, Czech Post does not execute direct debit payments from current accounts.

Set up/change/cancellation of TPRZ and TPI is not possible.

6.4 Deposit accounts

6.4.1 Deposit accounts - Corporate Clients

Transaction types	Time of transaction entry	Date of order submission for processing
Open deposit account	Any time during the business day from 0:00 to 24:00. If the entry is made on a weekend or holiday, the application defaults the date to the next business day.	D
Change revolving deposit account	Any time during the running cycle of the deposit (C), no later than one day before the maturity or deposit renewal. During the business day from 0:00 to 24:00.	On the deposit maturity or renewal day. Changes are valid for the next cycle of the deposit (C+1).
Change revolving deposit account	Any time during the deposit renewal day from 0:00 to 24:00.	After the expiry of the next deposit cycle on the deposit maturity or renewal day. Changes are valid for the next cycle of the deposit (C+2).
Terminate revolving deposit account*	Any time during the running cycle of the deposit (C), no later than one day before the maturity or deposit renewal. During the business day from 0:00 to 24:00.	Change of account type takes immediate effect.
Terminate revolving deposit account*	Any time during the deposit renewal day from 0:00 to 24:00.	On the deposit maturity or renewal day. Changes are valid for the next cycle of the deposit (C+1).

Money on a deposit account may be handled only via a business point and only on the maturity date or deposit renewal date.

It is not possible to execute changes or terminate a single-deposit account type via BUSINESS 24.

* Termination of a revolving deposit account is executed by a change of the account to the single-deposit account type.

6.4.2 Deposit accounts – Business Clients

Transaction types	Time of transaction entry	Date of order submission for processing
Open/change deposit account	Business day before 11:00 p.m.	D
Open/change deposit account	Business day after 11:00 p.m.	D+1

6.5 FX operations

6.5.1 FX operations

Types of FX operations	Time of transaction entry	Date of order submission for processing
Entry of single FX operations (Spot, Forward, Swap)	Business day from 8:00 a.m. to 5:30 p.m.	D+0 to D+365
Entry of single FX operations (Spot, Forward, Swap)	Business day after 5:30 p.m. and weekends	Operation cannot be entered
Entry of block FX operations (Spot, Forward, Swap)	Business day from 8:00 a.m. to 5:30 p.m.	D+0 to D+365

Types of FX operations	Time of transaction entry	Date of order submission for processing
Entry of block FX operations (Spot, Forward, Swap)	Business day after 5:30 p.m. and weekends	Operation cannot be entered
FX orders	Business day from 8:00 a.m. to 5:30 p.m.	D+0 to D+30 as per the conditions of entry
FX orders	Business day after 5:30 p.m. and holidays	Operation cannot be entered

General information

Orders/payments entered on a weekend or holiday or on a day before a weekend or holiday after 10:00 p.m. for corporate clients, after 11:00 p.m. for business clients will be handed over for inter-bank posting on the first business day following the day of entry.

Orders/payments entered on a day before a weekend or holiday before 10:00 p.m. for corporate clients, before 11:00 p.m. for business clients with a due date D+1 and D+2 (e.g. (Spot) will be executed on the first and second business day following the last non-working day, without being changed to another type of order.

Where payment transactions (apart from standing payment orders, standing direct debit orders, direct debits and deposit accounts) are co-authorised in BUSINESS 24, and the due date of the transaction expires while waiting for co-authorisation, it is possible to update this date by adding the remaining co-authorisation within thirty days of the due date and to execute the transaction with the current due date. After thirty days, the order becomes invalid and has to be re-entered. If, in the case of standing payment orders, standing direct debit orders, direct debits and deposit accounts the due date of the transaction expires while awaiting co-authorisation, the transaction becomes invalid and has to be re-entered.

In the case of orders entered via order batch import with potential retrospective due date in the batch, the order due date will be automatically updated to the current business day during the batch import.

In the case of payments (this applies to domestic payments, foreign-currency payment within the bank, domestic payment import and multiple domestic payments) with a due date entered as a non-business day, the due date will be changed to the next working day and the user will be informed of this change by the following message: “The due date has been amended to the next working day”.

The BUSINESS 24 IB service also offers an overview of transaction statuses for you. Transactions are classified into five categories: non-performed transactions, performed and deferred transactions, transactions awaiting further co-authorisation in the repository, and transactions for deletion in the repository. For corporate clients, non-performed or deferred transactions also display the reason why the transaction has not been executed.

Clients may additionally cancel transactions entered with a future due date and for corporate clients also transactions deferred due to lack of funds on the account.

Foreign payments, SEPA payments and payments from foreign-currency accounts entered with a future due date via BUSINESS 24 cannot be cancelled on the due date.

In all other cases it is not possible to cancel transactions additionally via BUSINESS 24.

Should you be uncertain about any postings of entered orders or payments it is necessary to contact the telephone support of the BUSINESS 24 service.

For all transactions, the transaction reference number will be automatically displayed in BUSINESS 24. The client can use this number for transaction identification (e.g. in a statement) or it will facilitate any potential complaint in respect of a transaction entered via BUSINESS 24.

The BUSINESS 24 IB service also allows for the sending of e-mail confirmations about accepted transactions, about transaction history, account details etc. These documents are also of an informative nature. The transfer of data is carried out in a standard manner, without any special security features, and therefore the bank cannot guarantee that they will not be obtained by a third person on the way from the bank to the client.

BUSINESS 24 is also equipped with a control function checking for unwanted duplicities of domestic transaction entries. When executing a domestic payment, a multiple domestic payment or orders import, the BUSINESS 24 service checks the transactions previously entered on the same day and if it identifies an identical transaction entered by any of the joint holders in respect of the given account, it will display a warning. The user may then check the previously entered transactions and cancel the entered transaction, or execute the transaction.

7. Use of BUSINESS 24

In addition to account management via internet banking, the BUSINESS 24 service offers also support communication with the telephone banker who will answer more complex questions and who may also carry out certain administrative operations associated with the administration of the account.

7.1 Via internet banking

The BUSINESS 24 service is available from the internet address **www.business24.cz** and allows for easy management of client accounts using clear menus and intuitive use of the application.

For a more detailed description of internet banking please refer to the BUSINESS 24 Help document, which is available from the login page under the link "Was your login unsuccessful?" and in the screen footer under the link "About the service".

When executing an active transaction, the service will always prompt the client to approve the transaction on a confirmation screen and to confirm by means of the Client Certificate.

7.2 Via telephone banker

Support for the BUSINESS 24 service is available on workdays between 7.00 a.m. and 6.00 p.m. at 956 777 888 (when calling from abroad: +420 956 777 888). After the welcoming message and language selection (CZ, EN) the client will be forwarded directly to a telephone banker

In case of accelerated authentication which requires disclosure of Client number and full name, the access is limited only to this offer of services:

- Account or joint holder set-up detail
- Transactions entered via BUSINESS 24.

In case of standard authentication, following the provision of the client number, password for Telebanking, and, upon first authentication in the SERVIS 24 Telebanking service, also selected positions from the security ID, the client will get access to a broader offer of services:

- Account or joint holder set-up detail
- Payment card detail
- Transactions entered via BUSINESS 24
- Transaction history
- Enquiry on the balance, and a number of other information.

8. BUSINESS 24 support

Should problems while using BUSINESS 24 be encountered, it is necessary to contact telephone support at the below provided numbers. Assistance with the following may be requested here:

- Problems with the Contract on the provision of BUSINESS 24
- Complications with accounts and cards assigned under BUSINESS 24
- Enquiries about BUSINESS 24 functionality
- Errors in BUSINESS 24 functionalities
- Technical problems with BUSINESS 24
- Problems with Client Certificate
- BUSINESS 24 set-up and installation
- Transaction complaints
- Balance enquiries
- Setting up passive access to an account
- Non-generated statements
- Client data inconsistencies (e.g. obsolete data in the bank systems).

Contact details:

- from fixed lines at: **956 777 888**
- from mobile phones: O2 at **726 118 128**
  T-Mobile at **605 661 128**
  Vodafone at **776 991 128**
- from abroad at: +420 956 777 888
- at e-mail address: **business24@csas.cz**

(Here it is possible to obtain answers to questions or send ideas regarding the BUSINESS 24 service)

The above-mentioned numbers may be called to request an answer to any queries on BUSINESS 24 and to contact the telephone banker with whose assistance it is also possible to perform certain administrative operations (see chapter 5.1 Authorised persons).

9. Implementing directive for the usage of electronic certificates in direct banking services

9.1 General provisions

A user purchasing a chip card reader undertakes to acquaint himself/herself with the licence terms ad conditions available from **https://www.csas.cz/PKILicence** and to observe them.

Certificates for the bank's purposes are issued by a certification authority. The certification authority is První certifikační autorita, a.s., Prague 9, Libeň, Podvinný mlýn 2178/6, Postal code 190 00, Company reg. no.: 26439395 incorporated under the Registry Court in Prague, Section B, item 7136 (hereinafter also referred to as I.CA). Information on the certification authority may be obtained from http://www.ica.cz, or from the following e-mail addresses: oper@ica.cz and info@ica.cz.

The user shall be obliged to verify the correctness of the certificate after the certificate is generated without unnecessary delay. If the user identifies inconsistencies between the Client Certificate content and data in the Protocol/Application, he/she shall be obliged to invalidate the certificate and to forthwith advise the bank to this effect.

The certificate shall be stored in the chip card and it shall be intended for securing direct banking services. The bank does not provide support for the use of the certificate outside the applications of direct banking services.

The certificate secures:

- Data integrity
- Obligation to provide response
- Confidentiality of data
- Set-up of a shared secret (key) within the protocol for secure data exchange
- Direct encryption and decryption of data
- Direct signing of data.

9.2 Validity and effect of electronic certificates and chip cards

The validity of electronic certificates has been set to the period of one year of the day of its issue by the certification authority.

Information on the period of validity of the Client Certificate with the specification of exact time point of certificate expiry may be obtained any time during its use,

- from the footer of BUSINESS 24 screens,
- from the Settings tab, under My settings,
- via certificate administrator,
- from the BUSINESS 24 line (tel. 956 777 888),
- from the Regional Corporate Centre or from another business point.

Throughout its validity the electronic certificate is in effect, i.e. it may be used to secure direct banking services as defined in this Manual. The possibility to use services requiring the use of an electronic certificate is linked to its validity and effect.

Client Certificate

Client Certificate invalidation, renewal or change of data therein is described in detail in chapter 3 BUSINESS 24 security of this Manual.

System Certificate

If the client requires securing direct banking services by system certificate, he/she may, after having signed an amendment to the contract on the use of direct banking services, generate an application with a password to obtain a system certificate. The bank does not issue, invalidate or renew/prolong system certificates. The client may use a system certificate by registering the system certificate in the direct banking services.

The bank does not provide software or support for the implementation and use of system certificate on the part of the client.

The use of system certificate security applies solely to the BUSINESS 24 Databanking direct banking service.

Software certificate

This is a necessary prerequisite for function of the BUSINESS 24 Mobile Bank service. This certificate is issued by Česká spořitelna, a.s. Certificate is provided free of charge, with one-year validity. Obtaining of the certificate is subject to a separate contract.

Chip card

For technical reasons, the validity of the chip card is limited. The expiry date is provided on the chip card in the YYYY format, which applies to December 31 of the given year. The last valid certificate may be downloaded to the chip card no later than on December 31 of the year preceding the expiry date of the chip card.

9.3 Electronic certificate validity renewal

Client Certificate

The validity of a user's Client Certificate may be renewed throughout its effective period, providing the following conditions are met:

- An effective contract on higher type of security has been concluded between the user and the bank and the user has not advised any change to his/her identification details specified in the protocol/application
- The user completes and submits an application for renewal via the certificate administrator in a manner allowing the bank to receive it before the Client Certificate expires.

Although the renewal of the Client Certificate means the issue of a new one, the current contract on higher type of security will remain in effect in this case and once the certification authority successfully issues the Client Certificate, the previous certificate will be automatically invalidated.

The bank will advice the client of the expiry of the Client Certificate at least one month before the end of its standard validity, through the BUSINESS 24 screen and, concurrently, by an e-mail message sent to the e-mail address specified in the protocol/application.

The bank shall decline Client Certificate renewal if the user does not have his/her own account activated for direct banking services and he/she is not a sponsored person. The user will be advised of this fact when submitting the application for Client Certificate prolongation.

System Certificate

The renewal of the system certificate via direct banking services is not supported by the bank. The client may apply for the issue of a new system certificate.

Software certificate

Software certificate is automatically renewed. If the client enters an active transaction within the interval of 30 – 90 days prior to the certificate expiry the request for a new certificate will be generated. Upon the next active transaction the certificate will be downloaded. If the client does not enter any active transaction within the interval of 30 – 90 days prior to the certificate expiry but only in the interval of 0 - 30 days, the client will be prompted to enter the password for secure repository immediately after the login and the certificate request will be created and the certificate downloaded. Until the certificate is successfully downloaded, the client cannot use the application. If the certificate expires, the client has to deactivate its device in the IB and to re-generate the single-use code and password for the MobileBank.

9.4 Electronic certificate issue

Client Certificate

In the following cases the user may/must apply for the issue of a subsequent (new) Client Certificate at a business point by submitting the application:

- The Client Certificate issued on the basis of the protocol and concluded contract on higher type of security or a previous application has expired, i.e. the user has not availed of the option to renew the Client Certificate
- If a change to the user identification details occurs (name/surname/address of permanent residence), even during the time of validity of the Client Certificate issued on the basis of the original identification details
- Loss/damage/exchange of the chip card or change of e-mail address.

The bank does not support the issuance of a subsequent Client Certificate for data which applied to a previously issued/invalidated Client Certificate.

System Certificate

The client applies for the issue of a subsequent (new) system certificate with I.CA. Before visiting I.CA, the client has to generate the electronic application for system certificate proper in the BUSINESS 24 Internetbanking application. The application does not support the generation of the application for the primary chip card. To be able to generate the application, the client has to have a valid secondary chip card allocated. The secondary chip card may be applied for by the owner of the BUSINESS 24 service or by the authorised person at a business point.

Software certificate

Certificate is issued at the first-time login into the application where the client is prompted to create a password for the certificate (secure repository). A request for certificate is generated and the certificate is downloaded to the mobile device. In the event of unsuccessful download the client can continue working in the application, however, without an option to submit active transactions. The certificate will be downloaded at the next login.

9.5 Electronic certificate invalidation

Client Certificate

The Client Certificate may be invalidated upon request of the user or in cases when the bank is entitled to invalidate the Client Certificate:

- The Client Certificate has been issued on the basis of untrue or falsified data or the validated and certified data are no longer valid and the bank learns about this fact
- The user failed to pay the price for the issue of the Client Certificate or has breached any obligation implied by the contract on higher type of security
- The user has died and the bank learns about this fact
- Automatically, when the contract on higher type of security expires and the user has been using security via Client Certificate or if a subsequent (new) Client Certificate has been issued upon application submission
- Automatically, when the client has advised a change of data to the Client Certificate and has not applied for a follow-up (new) client certificate within the established timeline
- The issuance of Client Certificates for the purposes of the bank has been terminated
- If concerned authorities have decided about the invalidation in compliance with effective legal regulations
- The user shall be entitled to invalidate his/her Client Certificate solely via certificate administrator or via the BUSINESS 24 line (tel.: 956 777 888 – the user will provide his/her name, surname and birth number).

The user shall be obliged to invalidate the Client Certificate if he/she suspects that it has been abused or if his/her chip card is lost or stolen.

After the bank receives the client's justified application for Client Certificate invalidation, it shall forthwith revoke the validity of the Client Certificate and since that moment it will not be possible to use the certificate for internet and telephone banking and the certificate shall be invalidated by the certification authority.

The invalidation of the Client Certificate irrevocably terminates its validity and it is no longer possible to use the certificate.

System Certificate

The bank does not support the invalidation of the system certificate via internet and telephone banking, but the client may use the direct banking services to enter a ban on the use of a system certificate allocated to his/her contract on the use of direct banking services. The revocation of validity of the system certificate is provided by I. CA.

Software certificate

Software certificate alone cannot be invalidated. In order to invalidate the certificate the BUSINESS 24 Mobile Bank service has to be deactivated.

10. Overview of operations in the BUSINESS 24 service

The overview specifies individual operations by the user rights and the communication channels through which the operations may be executed. Some of the operations associated with account administration do not need to be necessarily conducted directly at the business point, but they can be executed by phone through the BUSINESS 24 support lines (chapter 8 BUSINESS 24 support refers) or via the internet.

Joint holder/User administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Application for additional sending of new security data (security ID and Telebanking password)	✓	✓	✓	✓	✓		TB
Application for the generation of a new password for the obtaining of the certificate and the sending of the PKI mailer	✓	✓	✓	✓	✓		TB
Certificate renewal or change	✓	✓	✓	✓	✓		IB, RKC, P
Unblocking of password for BUSINESS 24 Internetbanking	✓	✓	✓	✓	✓		TB, IB[5]
Contract blocking					✓		TB, RKC, P,IB
Contract unblocking					✓		TB, RKC, P ,IB
Login SMS	✓	✓	✓	✓	✓		IB
User blocking	✓	✓	✓	✓	✓		TB
User unblocking	✓	✓	✓	✓	✓		TB
Application for the sending of a chip card	✓	✓	✓	✓	✓	Available only if chip card expires	IB, TB
Certificate collection	✓	✓	✓	✓	✓		IB
Use of certificate	✓		✓		✓	P, T only if the obligation to login via Client Certificate has been set up for them	IB
Revocation of (own) certificate validity	✓	✓	✓	✓	✓		IB, TB

Joint holder/User administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
User access to service					✓		IB
Login via client number and password	✓	✓	✓	✓	✓	Unless the obligation to log in via higher security has been set up for the joint holder	IB, TB
Setting up of access to data					✓		IB
Setting up of bank message sending	✓	✓	✓	✓	✓		IB
User administration					✓		IB
User administration – set-up of authorisations for activities					✓[6]		IB
Sponsored persons administration					✓		IB, TB
Change of password	✓	✓	✓	✓	✓		IB
Change of Telebanking password	✓	✓	✓	✓	✓	A joint holder without higher security will perform the change only via the voice automaton	IB
Change of contact details	✓	✓	✓	✓	✓		IB
Change of PIN for chip card	✓	✓	✓	✓	✓		IB
Unblocking PIN for chip card	✓	✓	✓	✓	✓	May be unblocked using PUK either on the login screen or immediately after blocking	IB
Mobile Bank set-up	✓	✓	✓			Obligation to log in	IB

Joint holder/User administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
						through Client Certificate	

Account administration	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Adding an account for management					✓		IB
Removing an account from management					✓		IB
Setting up account limit					✓		IB
Setting up co-authorisation limit					✓		IB
Setting up co-authorisation					✓		IB
Setting up the sending of the current FX rate table	✓	✓	✓	✓	✓		IB
Account name entry					✓		IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Entry of a single FX deal (Spot, Forward, Swap)[C]	✓	✓	✓		✓	AP + JH[4]	IB
Entry of block FX deal (Spot, Forward, Swap)[C]	✓	✓	✓		✓	AP + JH[4]	IB
FX order entry	✓	✓	✓		✓	AP + JH[4]	IB
List of open deals	✓				✓	An A right in respect of at least one account	
Entry of a SEPA payment	✓			✓		The payment may be entered with priorities as follows: Normal, Express, Prieuro	IB, RKC, P, DB, MBK

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Entry of a foreign payment (foreign payment system - ZPS)	✓			✓		The payment may be entered with priorities as follows: Normal, Urgent, Express	IB, KRC, P, DB
List of FX operations display	✓	✓	✓		✓	AP + JH[4]	IB
Entry of a direct debit order	✓			✓			IB, DB[1]
Entry of a transaction for co-authorisation (domestic payment^, multiple domestic payment^ foreign payment/SEPA^, Payment from FX, import of domestic payment/direct debit^, foreign payment/SEPA^)	✓			✓			IB
Entry of a payment from the account in a foreign currency	✓			✓			IB, DB
Entry of a payment from the account in CZK[1]	✓			✓			IB, DB, MBK
Cancellation of transaction with a future due date or of a transaction deferred due to lack of funds on the account [3]	✓						IB
Display of a direct debit	✓	✓		✓			IB
Direct debit detail	✓	✓		✓			IB
Setting up a direct debit[1]	✓			✓			IB, RKC, P
Change of direct debit[1]	✓			✓			IB
Cancellation of direct debit[1]	✓						IB
Display of a direct debit standing order	✓	✓					IB
Direct debit standing order detail	✓	✓					IB
Setting up a direct debit standing order[1]	✓						IB, RKC, P
Change of direct debit standing order[1]	✓						IB
Cancellation of direct debit standing order[1]	✓						IB
Display of standing order for balance adjustment	✓	✓		✓	✓	[7]	IB
Standing order for balance adjustment detail	✓	✓		✓	✓	[7]	IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Setting up a standing order for balance adjustment	✓				✓	AP has to be also joint holder "A" for the given client's account. [7]	IB, RKC, P
Change of a standing order for balance adjustment	✓				✓	AP has to be also joint holder "A" for the given client's account. [7]	IB
Cancellation of a standing order for balance adjustment	✓				✓	AP has to be also joint holder "A" for the given client's account. [7]	IB
Display of a standing payment order	✓	✓		✓			IB
Standing payment order detail	✓	✓		✓			IB
Setting up a standing payment order [1]	✓			✓			IB, RKC, P
Change of a standing payment order [1]	✓			✓			IB
Cancellation of a standing payment order [1]	✓						IB
Entry of multiple domestic payment from a CZK account [1]	✓			✓			IB
Above-limit withdrawal advice [1]	✓						IB
Export of data statements in the ABO or CSV formats for several accounts		✓					IB
Export of MT940 statements		✓					IB
Export of data statements in the xml format		✓					DB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
SEPA error statuses		✓				The XML files where you can find information on not performed SEPA payments/direct debits. The format complies with the version PAIN.002.001.03, approved by the European Payments Council.	IB, DB
Multiple deletion of orders from a batch[1]	✓			✓			IB
Import of a domestic payment/direct debit batch (ABO format or MC format)	✓			✓			IB
Import of a domestic payment/direct debit batch from several accounts of the payer at one time[1]	✓			✓			IB
Import of a foreign payment/ SEPA batch[1]	✓			✓			IB
Import SEPA batch in xml	✓			✓			IB, DB
Display of a text account statement and its export		✓					IB
Display of an electronic account statement and its export		✓					IB
Display of the account balance		✓					IB, DB
Activate/deactivate/change statement series					✓		IB
Payee templates (set-up, change, cancellation, use and export thereof)	✓			✓	✓		IB
Template download	✓	✓	✓	✓	✓		IB
Template import	✓			✓			IB
Application for the set-up/change of a current account					✓		IB, RKC, P
Account management with passive access[1]		✓					IB
Display of transactions for co-authorisation	✓	✓	✓	✓	✓		IB
Setting up the sending of credit advices					✓		IB

Current account	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Setting up the sending of text statements – Activation / Deactivation / Change[2]					✓		IB
Display of the list of advices		✓					IB
Transaction co-authorisation			✓				IB
Entry of a transaction for co-authorisation (domestic payment, multiple domestic payment, foreign payment, SEPA, batch import)				✓			IB
Display of the transaction history		✓					IB, DB
Display of the list of transactions entered via B24	✓	✓	✓	✓			IB
Confirmation of acceptance of transaction for processing	✓		✓	✓			IB
List of files sent for collection account		✓					IB
Sending of files (payments/direct debits) to the collection accounts[1]	✓			✓			IB
Display of the list of pending transactions	✓	✓					IB

Deposit and savings accounts	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Display of the deposit account	✓	✓		✓	✓		IB
Display of the savings account	✓	✓		✓	✓	[7]	IB
Deposit account detail	✓	✓		✓			IB
Savings account detail	✓	✓		✓		[7]	IB
Opening of a deposit account	✓				✓	AP has to be also joint holder "A" for the client's current account[3]	IB, RKC, P
Change of a deposit account		✓			✓	AP with P rights for the specific deposit account[3]	IB, RKC, P
Termination of a deposit account		✓			✓	AP with P rights for the specific deposit account[3]	IB, RKC, P

Payment cards and card accounts	Joint holder K	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Payment card detail			✓				Payment card holder: his/her own payment card only. Via TB also without authentication after the provision of certain personal data, only for private payment cards.	IB, TB
Card account detail			✓					IB, TB
Card account transaction history			✓					IB, TB
Payment card limit change	✓						Corporate clients only. Via the authorised person for everybody and	IB, TB

Payment cards and card accounts	Joint holder K	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
							payment card holder: his/her own payment card only, if they are listed at the specimen signature	
Change of payment card parameters and purchase of insurance	✓							IB
Display and change of card password	✓							IB
Payment card blocking								IB
Order of a replacement card	✓							IB
Payment card unblocking	✓							IB
List of blocked payment cards display	✓							IB
Temporarily active cards display	✓							IB

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Import of list of receivables to be pledged[6]	✓			✓		[7]	IB
List of receivables to be pledged[6]		✓				[7]	IB

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Application for loan drawdown					✓	Available only if at least one active loan account assigned under B24 exists[3] [7]	IB, RKC, P
Application for provision of a bank reference about the person					✓	[7]	IB, RKC, P
Application for the issue of a debit card					✓		IB, RKC, P
Application for the issue of cheque forms					✓		IB, RKC, P
Display of the list of bank guarantees[6]		✓				[7]	IB
Display of the list of overdraft loans		✓				[7]	IB
Display of the list of products within a credit line		✓				[7]	IB
Display of the list of credit lines		✓				[7]	IB
Loans		✓				[7]	IB
List of loans		✓				[7]	IB
Application for loan drawdown[6]	✓		✓	✓		[7]	IB
Exchange of documentation [6]	✓					[7]	IB
List of documents [6]	✓					[7]	IB
Free application[6]	✓		✓	✓		[7]	IB
File submission[6]	✓		✓	✓		[7]	IB
List of conditions of loan relationships to be fulfilled	✓				✓	[7]	IB
List of issued guarantees/letters of intent[6]	✓			✓	✓	[7]	IB
Issued guarantees[6]	✓			✓		[7]	IB
Advised guarantees[6]	✓			✓		[7]	IB
New transaction/bank guarantees[6]	✓			✓		[7]	IB
Data update[6]	✓			✓		[7]	IB
List of sent orders prior to 28 April 2014[6]	✓			✓		[7]	IB
Export letters of credit[6]	✓			✓		[7]	IB
Import letters of credit[6]	✓			✓		[7]	IB
Export collections[6]	✓			✓		[7]	IB
Import collections[6]	✓			✓		[7]	IB

Financing	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
New transaction[6]	✓			✓		[7]	IB
Data update[6]	✓			✓		[7]	IB
List of sent applications prior to 28 April 2014[6]		✓		✓		[7]	IB

PAYMENT 24	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Display of shopping basket detail		✓				Available only if an active account for PAYMENT 24 assigned under B24 exists	IB, DB

Information	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
List of financing products	✓	✓	✓	✓	✓		IB
Display of the summary list of accounts	✓	✓	✓	✓	✓		
Display of the list of accounts	✓	✓	✓		✓		IB, DB
Display of the account detail		✓					IB
Information on current loan burden of the client		✓					IB
Display of the current FX rates table		✓			✓		IB
Display of the setting of BUSINESS 24	✓	✓	✓	✓	✓		IB
Display of the current bank messages	✓	✓	✓	✓	✓		IB
Display of messages to be handled	✓	✓	✓	✓	✓		IB
Settings wizard					✓	Login via Client Certificate	IB

Exchange of documents	Joint holder A	Joint holder P	Joint holder E and S	Joint holder T	Authorised person	Comment	Communication channels
Send templates					✓		IB
Application for certificate	✓	✓	✓	✓	✓		IB
Display of the list of documents sent via B24 IB					✓		IB

[1] Transactions entered by type T joint holder require co-authorisation.

[2] Only for business clients.

[3] Only for clients included in the corporate clients.

[4] A user with the account owner profile (AP + JH), who works in the context of an accredited client.

[5] Only in cases of login through the Client Certificate

[6] Such authorisations for activities are set up by the selected authorised person. The special authorisation of the authorised person is stipulated by the contract.

[7.] Corporate clients only.

[^] The transaction entry date may be updated by adding the remaining authorisation and the transaction may be executed with the current date within thirty days of the due date expiry.

[B] Transactions for this purpose are: payment orders, batch import.

[C] Sending to so called administrative operations repository does not apply to the transactions.

The current version of the BUSINESS 24 user manual is available from the website of the bank (www.csas.cz, under the Downloads section).

11. List of terms and abbreviations

B24 – BUSINESS 24
C – Current (running) cycle (period) of deposit on a deposit account
FX – Foreign currency
D – Current business day (when the date of transaction entry is a business day) or the first business day after the entry of the transaction (when the transaction entry date is not a business day)
DB – BUSINESS 24 Databanking
FOO – Natural person- private individual
FOP – natural person - entrepreneur
HPÚ – Multiple payment order
IB – Internetbanking
IVR – Automatic voice response service
PI – Direct debit order
PÚ – Payment order
DP – Domestic payment
HDP – Multiple domestic payment
RKC – Regional Corporate Centre of ČS, a.s.
P – A branch of ČS, a.s.
PO – Legal person
SI – Direct debit
STP – "Straight-through processing" = a cross-border transfer as referred to by the Regulation of the European parliament and Council (EC) no. 2560/2001 is a payment in EUR to EU and EEA countries with specified IBAN and BIC code, with fees disposition SHA and without further instructions from the client.
SEPA – "Single Euro Payment Area" - SEPA is a uniform area for the execution of payments in EUR. SEPA includes countries of the European Economic Area (EU countries + Norway, Lichtenstein, Iceland) and Switzerland. It contains new additional fields which allow for a better identification of the payment for the payer and for the payee (optional fields).
TB – Telephone banker
TPI – Standing direct debit order
TPRZ – Standing order for balance adjustment
TPÚ – Standing payment order
VÚ – Deposit account
ÚÚ – Loan account
ZP – Foreign payment

Administrative operation

An operation which results in a change to the set-up of the BUSINESS 24 service and user rights.

Accredited client

A client who has signed a contract or framework contract on dealing in financial markets with the Dealing unit and on the basis of the bank's business decision has been entered in the bank system allowing to offer this client individual terms and conditions for dealing in financial markets. The client is informed of such decision of the bank.

Active financial transaction

Transactions resulting in transfers of money.

Security ID

A number which is required particularly during first-time login to the BUSINESS 24 service and when unblocking a user. It is an eight-digit number provided in a security envelope.

Security data

Unique identifiers (client number, security ID, and Telebanking password), which are automatically allocated to each newly set-up user for the purposes of his/her unique identification for providing of access to direct banking services.

Security tools

Security features allocated by the bank to the user for the purposes of his/her identification and serving for the provision of access to direct banking services of the user using enhanced security of communication with the bank (e.g. the Client Certificate).

Security SMS

These include authorisation SMS messages (applies only to the services of SERVIS 24) and login SMS messages set up for the concerned user.

BUSINESS 24 Databanking
BUSINESS 24 Databanking is a data interface allowing the client who has activated the BUSINESS 24 service and who uses an accounting (ERP) or other system supporting Databanking, to avail of direct communication between this system and the bank. Usage has to be permitted by the bank.

Certification authority
An institution which issues administers and invalidates certificates.

Chip card
A secure repository of the certificate, an independent microprocessor on a card pursuant to ISO 7916.

Chip card reader
Hardware device necessary for the use of chip cards.

Electronic certificate
A data message issued to the client or authorised person by the certification authority which serves for the purposes of electronic signature generation, particularly of the identification and verification of identity of the acting client or authorised person.

Bank's financial group
Includes the bank subsidiaries (members of the Česká spořitelna Financial Group), a company which has decisive asset share in the bank (the bank's parent company) and companies where the bank's parent company has a more than 25% asset share of the registered capital or a share in excess of 25% of voting rights. Current information on the members of the Bank's financial group is available from the bank's website and at its business points.

Password for obtaining the certificate
A one-time password for the confirmation of the application for Client Certificate.

IVR
Automatic voice response service.

Client
An entity (natural person – private individual, natural person –entrepreneur, legal person) who concludes a contract with the bank and who is the owner of the primary account to which the BUSINESS 24 IB service is linked.

Client Centre Prostějov
(Also KCP) A workplace of the bank which provides, by means of phone, SMS messages or e-mail messages direct banking services (including their support) and information on products ands services of the entire Bank's group.

Client Certificate
An electronic certificate issued to the user of the SERVIS 24 / BUSINESS 24 services. The user uses it for authentication into the SERVIS 24 Internetbanking / BUSINESS 24 Internetbanking services and for the authorisation of transactions entered via the SERVIS 24 / BUSINESS 24 services. It is a commercial personal certificate issued by I. Certifikační autorita.

Commercial client
A client whose contract on the maintenance of current account states that he/she is maintained in the Commercial Clients group.

Mailing address
The address to which correspondence associated with the BUSINESS 24 service is sent to the user.

Non-accredited client
A client who has not signed a contract or framework contract on dealing in financial markets with the Dealing unit and has not been entered in the bank system allowing to offer the client individual terms and conditions for dealing in financial markets.

Business day
Any day when the bank and other banks in the Czech Republic are opened and when settlement of inter-bank deals is executed.

Business point
A branch, a regional corporate centre, or a headquarters unit (corporate clients, real estate and mortgages and municipal financing).

Passive transactions
Any information provided via the BUSINESS 24 service.

Payment card
A non-cash payment instrument. It includes all types of cards (debit card, credit card, additional credit card, charge card, prepaid card).

Signature specimen
A power of attorney form, where the client specifies the authorised persons (the client may include himself/herself among the authorised persons), signature specimen of these persons or the scope of their authorisation).

Primary account
An account to which the contract on the provision of the BUSINESS 24 service is related.

Protocol (also Higher-type security protocol)
A document drafted if the client is interested in obtaining the Client Certificate (a security tool) which is considered to be an invitation to act addressed to the bank for the purposes of concluding a higher-security contract (security tool).

Login SMS

A SMS message sent by the bank to the client to his/her mobile phone which contains a login SMS code.

Login SMS code
A numerical code contained in the Login SMS, which serves for the purposes of authorisation of security data when the client logs into the BUSINESS 24 Internetbanking service.

Co-authorisation
Additional confirmation of active transactions or administrative operations by other joint holders as per the set-up authorisations. A co-authorisation power may include a power of joint or separate co-authorisation. The signature of the joint holder authorised to perform separate co-authorisations replaces any number of joint holder authorisations with the power of joint co-authorisation.

Direct banking services
Services provided by the bank to the client within the scope of which the client may execute active and passive transactions and administrative operations via telephone, internet or other remote communication tools.

Contract
The contract on the provision of BUSINESS 24.

Contract on higher-type security
An agreement between the user and the bank on the basis of which the user is provided with a Client Certificate. It is a contract on the usage of a security tool as referred to by the respective item of the General business terms and conditions of Česká spořitelna, a.s.

Sponsor
A client of the BUSINESS 24 service to whose primary account prices as per the Česká spořitelna, a.s., pricelist are charged for bank deals associated with user administration. Currently, a sponsor for the Client Certificate (e.g. renewal) and for e.g. repeated sending of security data is set up. In respect of a newly set-up user, the client on whose initiative the user is being set-up is automatically set up as the user's sponsor. This set-up may be changed by the authorised person.

Sponsored person
The user for whom the bank charges the fees and prices associated with the set-up and administration of security tools according to the Pricelist of Česká spořitelna, a.s. for bank deals to the account whose owner has agreed to such arrangement via direct banking services.

Certificate administrator
Software, internet application allowing for the administration of the Client Certificate.

System certificate
An electronic certificate registered for the contract on BUSINESS 24 for use with BUSINESS 24 Databanking. It serves for the authentication of the server or system which executes automated operations. It is a commercial server certificate issued by I. Certifikační autorita.

Telephone banker
An employee of Client Centre Prostějov, who provides the predefined scope of services of the Bank's group to both authenticated and non-authenticated users via phone.

User
A natural person (holder of security data) who has logged in to the BUSINESS 24 service via the correct security data.

User – Authorised person (also authorised person)
A user acting on behalf of the client on the basis of authority specified in respect of him/her in the contract.

User – Joint holder (also joint holder)
A user who is authorised to handle money on the client’s accounts on the basis of an authority and within the scope assigned by the user - authorised person thereto. A joint holder has to be specified in the valid specimen signature for the concerned account.

Credit line
A credit scope of a predefined amount which includes one or more loan products.

Application (also application for higher-type security).
A document specifying the client's requirement addressed to the bank for the change of identification data associated with a security tool/Client Certificate.